UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/020,524	12/14/2001	Katharina Veronika Koelle	50040.01USU1	9082

7278 7590 09/27/2005

DARBY & DARBY P.C.
P. O. BOX 5257
NEW YORK, NY 10150-5257

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/020,524	KOELLE ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/22/02, 7/29/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1- 27 are pending for examination.

2. Claims 1- 20, 22-27 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1- 20, 22-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Wohlgemuth et al, U.S. Patent Application publication US 2002/0087883 A1.

4. As per claim 1; "A method of protecting machine readable media from unauthorized storage or copying, comprising:

sending a detector to a client process [para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications per se being streamed to the client from the server for subsequent processing prior to execution, and, the said applications inclusive of filtering file accesses (i.e., a detector; '... fine grained filtering of file accesses directed at remotely served files...'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

receiving a response to the detector from the client process [para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution, and, the said applications inclusive responding with a communications back to the server (i.e., licensing/licensing server processing concerned with authorized software installation and use), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

detecting a presence of an unauthorized software behavior on the client based upon

the response and

a matching rule that is associated with the detector sent [para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution, and, the said applications inclusive responding with a communications back to the server (i.e., figure 40 and associated description; licensing/licensing server processing concerned with authorized software installation and use), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

updating a database of detectors for

a previously unseen and unauthorized behavior of the process such that

the database of detectors evolves over time [para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution, and, the said applications inclusive responding with a communications back to the server (i.e., licensing/licensing server processing concerned with authorized software

installation and use, whereas the licensing and associated authorization to use or how much to use (i.e., anti-piracy), etc., encompasses the '... updating a database ... unseen and unauthorized behavior of the process ... database of detectors evolves over time ...'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

As per claim 15, this claim is the broader claim aspect for the method claim 1 above insofar as this claim deals with '...series of behavioral questions ...' form of a client/server or client intra-process (i.e., multitasking aspects) request/response aspects of the application as detector, and is rejected for the same reasons provided for the claim 1 rejection; "A method of providing detection of machine-readable media from an unauthorized usage, the method comprising:

evaluating a response from a process to

a series of behavioral questions;

detecting an unauthorized behavior of the process based on

the evaluating; and

communicating the unauthorized behavior of the process among

a plurality of processes,

wherein detection of unauthorized usage is enhanced.".

As per claim 16, this claim is the apparatus/system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A system to protect media from unauthorized usage, the system comprising:

a server to send media to a client; and

a program to perform actions when executed that include:

sending a detector to the client,

receiving a response to the detector from the client,

detecting a presence of an unauthorized process on the client based on

the response and

a matching rule associated with the detector, and

updating a database of memory detectors for

a previously undetected and unauthorized process on the client such that

the database of memory detectors evolves over time.".

As per claim 23, this claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A machine readable medium that provides instructions which, when executed by at least one processor, cause said processor to perform operations comprising:

sending a detector to a client process;

receiving a response to the detector from the client process;

detecting a presence of an unauthorized behavior on the client based upon

the response and

a matching rule that is associated with the detector sent; and

updating a database of memory detectors for

a previously unseen and unauthorized behavior of the client process such that

the memory database evolves over time.".

5. Claim 2 ***additionally recites*** the limitation that; "The method as in claim 1, wherein the sent detector includes at least one of

a self-detector,

a memory detector, and

a novel detector.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the memory type where the application resides as related to the detection software functionality (i.e., para. 0082-0083, 0132-0163), communications back to the server (i.e., figure 40 and associated description; licensing/licensing server processing concerned with authorized software installation and use), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 24, this claim is the embodied software claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; "The medium as in claim 23, wherein

the detector further includes at least one of

a self-detector,

a memory detector, and

a novel detector.".

6. Claim 3 ***additionally recites*** the limitation that; "The method as in claim 1, wherein the sent detector further comprises

detecting the presence of

an unauthorized substantially simultaneously executing client process.". The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the multitasking '... substantially simultaneously executing client process ...' Windows/UNIX/Internet browser applications/environments such that execution of the associated processes/sub processes, threads, etc., inherent in such environments, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 25, this claim is the embodied software claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "The medium as in claim 23, wherein

the detector detects the presence of

an unauthorized substantially simultaneously executing client process.".

7. Claim 4 ***additionally recites*** the limitation that; "The method as in claim 1, wherein the sending of the detector further comprises

varying a sequence length of a computer system call within the detector such that the meaning of the detector is obscured.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources whereas the parameters used in the call are inherently application specific (i.e., the number of parameters, and format thereof), and, in the case of the detector file access functionality '... varying a sequence length ... call ... detector is obscured ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 26, this claim is the embodied software claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection; "The medium as in claim 23, wherein

the sending of the detector further includes

varying a sequence length of computer system calls within the detector such that the meaning of the detector is obscured.".

8. Claim 5 ***additionally recites*** the limitation that; "The method as in claim 1, wherein the sending of the detector further comprises

encoding numerically the detector such that

the meaning of the detector is obscured.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources, in specified and predetermined format/protocols, whereas the parameters used in the call are inherently application specific (i.e., the number of parameters, and format thereof), and, in the case of the detector file access functionality '... encoding numerically the detector ... detector is obscured ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 27, this claim is the embodied software claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; "The medium as in claim 23, wherein

the sending of the detector further includes

encoding numerically the detector such that

the meaning of the detector is obscured.".

9. Claim 6 ***additionally recites*** the limitation that; "The method as in claim 1, wherein the matching rule includes

a criterion for each field in the detector that is to be matched before a match is validated,

wherein each field includes

a sequence of at least one computer system calls.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources, in specified and predetermined format/protocols, whereas the parameters (i.e., encoded as data fields) used in the call are inherently application specific, and, in the case of the detector file access (i.e., read, write, modify, attribute change/edit, etc.,) functionality '...criterion ... field ... match ... validate ... sequence ... system calls ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 22, this claim is the embodied software claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; "A computer readable medium having stored thereon a data structure to provide a detector pattern for use in data integrity of machine-readable media, the data structure comprising

a plurality of data fields associated with

a matching rule to validate a match of

the plurality of data fields from

a response to the data structure, and

wherein each of the plurality of data fields comprises

a computer system call.".

10. Claim 7 ***additionally recites*** the limitation that; "The method as in claim 1, further including

sending the detector to detect

previously unseen and unauthorized behavior to another client process.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution, and, the said applications inclusive responding with a communications back to the server (i.e., licensing/licensing server processing concerned with authorized software installation and use, whereas the licensing and associated authorization to use or how much to use (i.e., anti-piracy), etc., encompasses the '... sending the detector to detect ... unseen and unauthorized behavior of the process ...'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

11. Claim 8 ***additionally recites*** the limitation that; "The method as in claim 1, further including:

exchanging sets of memory detectors between

a server and

another server during an update period;

evaluating the received set of memory detectors against

each server's self database and

a set of matching rules;

discarding memory detectors in the received set of memory detectors that match

another detector in each server's self database,

wherein a false positive detection is minimized; and

merging each new retained memory detector from

the received set of memory detectors with each server's memory database,

wherein the exchange of the sets of memory detectors between each server obstructs

the spread of unauthorized copying and corruption of electronic media.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution, and, the said applications inclusive responding with a communications back to the server (i.e., licensing/licensing server processing concerned with authorized software installation and use, whereas the licensing and associated authorization to use or how much to use (i.e., anti-piracy), etc., encompasses the server to server database updating/merging process insofar as the licensing/licensing server is embodied in a '... ASP server cluster [i.e., para. 0077] ...') and the advantages of such as taught, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

12. As per claim 9, this claim is claim 8 above as applied to a specific update period, whereas at the very least the applications subscription/licensing aspects deal with such limitations, and is rejected for the same reasons provided for the claim 8 rejection; "A method for obstructing unauthorized copying and corruption of media between clients that communicate over a network of servers, comprising:

exchanging a set of memory detectors between

servers during an update period;

evaluating each received set of memory detectors against

each server's self database and

a set of matching rules;

discarding each detector in the received set of detectors that match

another detector in each server's self database; and

merging a new retained detector from

each received set of detectors with each server's memory database,

wherein the exchanging of the set of memory detectors prevents

unauthorized copying and corruption of media.".

13. Claim 10 ***additionally recites*** the limitation that; "The method as in claim 9, wherein the set of detectors include at least one of

a self-detector,

a memory detector, and

a novel detector.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the memory type where the application resides, as related to the detection software functionality (i.e., para. 0082-0083, 0132-0163), inclusive of the response associated with the communications back to the server (i.e., figure 40 and associated description; licensing/licensing server processing concerned with authorized software

installation and use), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

14. Claim 11 ***additionally recites*** the limitation that; "The method as in claim 9, wherein the set of detectors enable the detection of the presence of

an unauthorized substantially simultaneously executing client process.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the multitasking '... substantially simultaneously executing client process ...' Windows/UNIX/Internet browser applications/environments such that execution of the associated processes/sub processes, threads, etc., inherent in such environments, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

15. Claim 12 ***additionally recites*** the limitation that; "The method as in claim 9, wherein the exchanging the set of memory detectors further includes

varying a sequence length of

a computer system call within each detector such that

each detector is obscured.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources whereas the

parameters used in the call are inherently application specific (i.e., the number of parameters, and format thereof), and, in the case of the detector file access functionality '... varying a sequence length ... call ... detector is obscured ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

16. Claim 13 ***additionally recites*** the limitation that; "The method as in claim 9, wherein the exchanging the set of detectors includes

encoding numerically the detector such that

the meaning of the detector is obscured.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources, in specified and predetermined format/protocols, whereas the parameters used in the call are inherently application specific (i.e., the number of parameters, and format thereof), and, in the case of the detector file access functionality '... encoding numerically the detector ... detector is obscured ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

17. Claim 14 ***additionally recites*** the limitation that; "The method as in claim 9, wherein the matching rule includes

at least one criterion for each field in each detector that is to be matched

before a match is validated, and

wherein each field includes

a sequence of at least one computer system calls.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources, in specified and predetermined format/protocols, whereas the parameters (i.e., encoded as data fields) used in the call are inherently application specific, and, in the case of the detector file access (i.e., read, write, modify, attribute change/edit, etc.,) functionality '...criterion ... field ... match ... validate ... sequence ... system calls ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

18. Claim 17 ***additionally recites*** the limitation that; "The system as in claim 16 further including

employing the client to access the media."

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the multitasking '... client to access the media ...' applications/environments such that execution of the associated processes/sub processes, threads, etc., interactively deals with the client access of the media (i.e., read, write, etc.,), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

19. Claim 18 ***additionally recites*** the limitation that; "The system as in claim 16, wherein the sending of the detector includes

adjusting the frequency of a class of detectors sent in response to

changes in responses from each client, such that

the class of detectors includes at least one of

a self-detector,

a memory detector, and

a novel detector.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the memory type (i.e., class) where the application resides, as related to the detection software functionality (i.e., para. 0082-0083, 0132-0163), inclusive of the response associated with the communications back to the server (i.e., figure 40 and associated description; licensing/licensing server processing concerned with authorized software installation and use), such that the licensing aspects of the application provide the dynamic frequency adjustment criteria to the detection, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

20. Claim 19 ***additionally recites*** the limitation that; "The system as in claim 16, wherein the updating further includes

eliminating detectors in the database that exceed

a predetermined detector life span.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the

server for subsequent execution, and, the said applications inclusive responding with a communications back to the server (i.e., licensing/licensing server processing concerned with authorized software installation and use, whereas the licensing and associated authorization to use or how much to use (i.e., anti-piracy), etc., encompasses the '...eliminating detectors in the database ... predetermined detector life span ...'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

21. Claim 20 ***additionally recites*** the limitation that; "The system as in claim 16, wherein the matching rule includes

at least one criterion for a field in the detector to be matched before a match is validated, and

wherein the field includes

a sequence of at least one computer system calls.".

The teachings of Wohlgemuth et al suggest such limitations (para. 0016-0021, 0072-0121, figures 1-45 and associated descriptions, whereas the applications sent to the client from the server for subsequent execution are inclusive of the calls to system resources, in specified and predetermined format/protocols, whereas the parameters (i.e., encoded as data fields) used in the call are inherently application specific, and, in the case of the detector file access (i.e., read, write, modify, attribute change/edit, etc.,) functionality '...criterion ... field ... match ... validate ... sequence ... system calls ...', clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

Allowable Subject Matter

22. Claim 21 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, as such; "The system as in claim 16, wherein

the detecting includes

executing a Rabin-Karp algorithm of prime numbers and

a sliding window across

the response and

the detector.".

Conclusion

23. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

Primary Examiner
AU 2131
9/23/05